

REMARKS

The above Amendments and these Remarks are in reply to the Office action mailed June 29, 2006. Currently, claims 1-57 are pending. Applicants have amended claims 1, 3, 7, 11, 13, 16-18, 31, 34, 36-37, 40-41, 49-51, 54, and 57. Applicants respectfully request reconsideration of claims 1-57.

I. Claim Rejections

Claims 1-57 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,689,566 (“*Nguyen*”).

II. Response to Rejection of Claims 1-17, 31-40, and 49-57

Because *Nguyen* fails to disclose each of the limitations of claims 1-17, 31-40, and 49-57, Applicants assert that these claims are patentable over the cited art.

Independent claims 1, 31, and 49 have each been amended, and now recite:

- (a) receiving log-in data for a client during a first log-in attempt;
- (b) authenticating said client, wherein said step (b) includes the steps of:
 - (1) applying a first function to a value in said log-in data to obtain a first result, and
 - (2) employing said first result in determining whether to authenticate said client during said first log-in attempt;
- (c) *completing said first log-in attempt;*
- (d) *automatically determining that said current security scheme is to be replaced by a desired security scheme after completing said first log-in attempt, wherein said determining is performed before a next log-in attempt for said client; and*
- (e) modifying at least one record in said computer system in response to said step (d) *before said next log-in attempt*, wherein said step (e) includes the step of:
 - (1) applying a second function to said value received in said step (a) to obtain a second result. (*Emphasis added*).

The amended versions of claims 1, 31, and 49 recite a technique for updating a current security scheme on a computer system. Steps of the claimed method include “authenticating said client” using log-in data received “during a first log-in attempt,” “completing said first log-in

attempt,” and “*automatically determining that said current security scheme is to be replaced by a desired security scheme after completing said first log-in attempt, wherein said determining is performed before a next log-in attempt for said client.*” In response to determining that the current security scheme is to be replaced, at least one record in the computer system is modified “before said next log-in attempt.” These concepts recited in independent claims 1, 31, and 49 are not disclosed by *Nguyen*.

First, *Nguyen* makes no determination that a “current security scheme is to be replaced by a desired security scheme,” as recited in claims 1, 31, and 49. The cited portions of *Nguyen* disclose a “logon procedure [that] uses a three way authentication.” *Nguyen*, col. 3, lines 40-45. A first step at the client computer “encrypts the very first logon packet with different keys for each part of the packet,” uses “a DES key to encrypt the user ID,” and “generates a key Ka from the user ID and password using a one way hash function.” *Id.* at col. 3, lines 41-67. A second step of the logon procedure takes place at the server which performs operations including decrypting the user ID, determining “if password Ka matches Kb,” and generating and encrypting “both random numbers Ra and Rb with the password before sending the first logon response packet to the client.” *Id.* at col. 4, lines 5-39. These steps are followed by a third step at the client, a fourth step at the server, and a fifth step at the client involving a second logon packet used as part of the logon procedure. *Id.* at col. 3, line 40-col. 4, line 26. There is no mention in these portions of *Nguyen* or elsewhere of “automatically determining that said current security scheme is to be replaced,” as recited in claims 1, 31, and 49.

Nguyen concludes by stating that after “the logon procedure is successfully completed, all session headers are encrypted using the session key Ks and the IV.” *Id.* at col. 4, lines 27-32. This portion of *Nguyen* clarifies that each of the five steps is part of the same logon procedure. Presumably, they are all performed according to the same security scheme as *Nguyen* makes no mention of replacing the security scheme at any point during the disclosed logon procedure. Accordingly, *Nguyen* does not disclose the concept of “automatically determining that said current security scheme is to be replaced by a desired security scheme,” as recited in claims 1, 31, and 49.

Second, *Nguyen* does not disclose “automatically determining that said current security scheme is to be replaced ...*after completing said first log-in attempt,*” and “*before a next log-in attempt for said client,*” as recited in claims 1, 31, and 49. *Nguyen*’s disclosed process is part of a

single log-in attempt or procedure as illustrated above. Thus, even if the steps are regarded as somehow disclosing the replacement of a security scheme (a point with which Applicants' strongly disagree), they would be performed as part of, and during a single "logon procedure." Therefore, there is no disclosure in *Nguyen* of "automatically determining that said current security scheme is to be replaced by a desired security scheme after completing said first log-in attempt," and "before a next log-in attempt for said client," as recited in claims 1, 31, and 49.

Finally, in a later portion of the disclosure *Nguyen* also describes various packets "as encrypted by security level 1," "encrypted by security level 2," or "encrypted by security level 3." *Id. at col. 9, lines 10-27*. This portion further illustrates that *Nguyen* does not disclose "automatically determining that said current security scheme is to be replaced by a desired security scheme after completing said first log-in attempt, wherein said determining is performed before a next log-in attempt for said client," as recited in claim 1.

Nguyen states that to "protect data exchanged over communication sessions, the preferred embodiment provides two different encryption schemes available to the user at logon." *Id. at col. 9, lines 28-30*. "Once an encryption scheme is selected, data exchanged over all sessions connected to a network domain are encrypted regardless of the communication protocol." *Id. at col. 3, lines 35-40*. Thus, rather than disclosing "automatically determining," as recited in claim 1, *Nguyen* discloses that different encryption schemes are available to the user for selection at logon. Moreover, it is clear from this discussion that the selection is part of a particular logon procedure. As such, any selection of a security scheme in *Nguyen* would not be "after completing said first log-in attempt," and "before a next log-in attempt for said client," as recited in claims 1, 31, and 49.

Because *Nguyen* fails to disclose each limitation of claims 1, 31, and 49, Applicants assert that these claims are patentable over the cited art. Claims 2-17, 32-40, and 50-57 each ultimately depend from claims 1, 31, and 49 respectively. Applicants respectfully submit that these claims are patentable over the cited art for at least the same reasons as claims 1, 31, and 49.

III. Response to Rejection of Claims 18-30 and 41-48

Because *Nguyen* fails to disclose each of the limitations of claims 18-30 and 41-48, Applicants assert that these claims are patentable over the cited art.

Independent claims 18 and 41 have each been amended, and now recite:

- (a) creating a log-in record at said intermediate system, wherein said log-in record includes a security identifier and a first encrypted value, wherein said security identifier corresponds to a current security scheme employed by said intermediate system;
- (b) receiving log-in data for said client;
- (c) *authenticating access of said client to said intermediate system*, based on data from said log-in data and data from said log-in record;
- (d) *obtaining authentication data to send to said primary system, wherein said authentication data includes data from a decrypted version of said first encrypted value at said intermediate system*;
- (e) determining that said current security scheme is to be replaced by a desired security scheme; and
- (f) modifying said log-in record, wherein said step (f) includes the steps of:
 - (1) updating said security identifier to correspond to said desired security scheme,
 - (2) employing data in said log-in data received in said step (b) to calculate a second encrypted value, and
 - (3) replacing said first encrypted value with said second encrypted value. (*Emphasis added*).

Independent claims 18 and 41 each recite “a method for providing a client with access to a primary system through an intermediate system.” The method includes “creating a log-in record *at said intermediate system*,” “*authenticating access of said client to said intermediate system*,” and “*obtaining authentication data to send to said primary system*, wherein said authentication data includes data from a decrypted version of said first encrypted value at said intermediate system.” The concept of authenticating a user at an intermediate system and obtaining authentication data to send to a primary system, as recited in claims 18 and 41, is not within the disclosure of *Nguyen*.

First, *Nguyen* does not disclose “authenticating access of said client to said intermediate system,” as recited in claims 18 and 41. As described above, the cited portions of *Nguyen* involve one “logon procedure” “to allow both the client and the server to authenticate each other.” *Id. at col. 3, lines 41-47*. *Nguyen* discloses that “the first step takes place at the client computer,” “the second step in the process takes place at the server,” “the third step in the process takes place at the client computer,” “the fourth step in the process takes place at the server computer,” and “the fifth step in the process takes place at the client computer.” *Id. at col. 3, line 51-col. 5, line 26*. *Nguyen* summarizes “the logon procedure” as follows (where C=client and S=server): “1. C to S; 2. S to C;

3. C to S; 4. S to C.” *Id. at col. 5, lines 63-67*. Thus, this process merely involves a client and server. There is no “authenticating access of said client to said intermediate system,” as recited in claims 18 and 41.

Second, *Nguyen* does not disclose “obtaining authentication data to send to said primary system, wherein said authentication data includes data from a decrypted version of said first encrypted value at said intermediate system,” as recited in claims 18 and 41. This limitation plainly requires that “authentication data to send to said primary system” be obtained from a version of “said first encrypted value at said intermediate system.” *Nguyen*’s disclosure only provides a logon procedure between client and server, as set forth in *col. 3, line 40-col. 5, line 35* and summarized at *col. 5, lines 63-67*. There is no disclosure that the authentication data for the server comes from some intermediate system as recited in claims 18 and 41.

In fact, *Nguyen* specifically discusses a feature of one implementation where “multiple servers can be connected together,” and states that “this feature requires the intermediate servers’ administrators to manually logon the designated servers *since the logon passwords are not stored on the intermediate servers*.” *Id. at col. 13, lines 55-60*. This language specifically states that logon passwords are not stored on the intermediate servers. Thus, there is clearly no disclosure in *Nguyen* of “obtaining authentication data to send to said primary system” from information “at said intermediate system,” as recited in claims 18 and 41.

Because *Nguyen* fails to disclose each limitation of claims 18 and 41, Applicants assert that these claims are patentable over the cited art. Claims 19-30 and 42-48 each ultimately depend from claims 18 and 41, respectively. Applicants respectfully submit that these claims are patentable over the cited art for at least the same reasons as claims 18 and 41.

IV. Conclusion

Based on the above amendments and these remarks, reconsideration of claims 1-57 is respectfully requested.

The Examiner’s prompt attention to this matter is greatly appreciated. Should further questions remain, the Examiner is invited to contact the undersigned attorney by telephone.

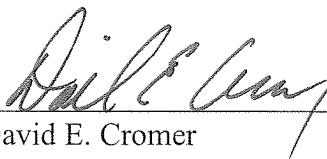
Enclosed is a PETITION FOR EXTENSION OF TIME UNDER 37 C.F.R. § 1.136 for extending the time to respond up to and including today, November 29, 2006.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 501826 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: November 29, 2006

By: _____



David E. Cromer
Reg. No. 54,768

VIERRA MAGEN MARCUS & DENIRO LLP
575 Market Street, Suite 2500
San Francisco, CA 94105-2871
Telephone: (415) 369-9660
Facsimile: (415) 369-9665